Atos Worldline
An Atos Origin Company

Haachtsesteenweg 1442
1130 Brussels
Belgium

DEP Documentation

CTAP Certificate Generation User Manual

Version Management Report

Version	Name(s)	Date	Comments
01.00	David Lheureux	10/05/2006	First version
01.01	David Lheureux	12/05/2006	After review.
01.02	David Lheureux	12/02/2007	Version 2.4 of CTAP Certificate Generation
04.00	Anna Papayan	25/03/2011	Change the template into Atos Worldline, minor changes.

CONFIDENTIALITY

The information in this document is confidential and shall not be disclosed to any third party in whole or in part without the prior written consent of Atos Worldline S.A./N.V.

COPYRIGHT

The information in this document is subject to change without notice and shall not be construed as a commitment by Atos Worldline S.A./N.V.
The content of this document, including but not limited to trademarks, designs, logos, text, images, is the property of Atos Worldline S.A/N.V. and is protected by the Belgian Act of 30.06.1994 related to author's right and by the other applicable Acts.
The contents of this document must not be reproduced in any form whatsoever, by or on behalf of third parties, without the prior written consent of Atos Worldline S.A./N.V.
Except with respect to the limited license to download and print certain material from this document for non-commercial and personal use only, nothing contained in this document shall grant any license or right to use any of Atos Worldline S.A./N.V.'s proprietary material.

LEGAL DISCLAIMER

While Atos Worldline S.A./N.V. has made every attempt to ensure that the information contained in this document is correct, Atos Worldline S.A./N.V. does not provide any legal or commercial warranty on the document that is described in this specification. The technology is thus provided "as is" without warranties of any kind, expressed or implied, included those of merchantability and fitness for a particular purpose. Atos Worldline S.A./N.V. does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product or process disclosed.
To the fullest extent permitted under applicable law, neither Atos Worldline S.A./N.V. nor its affiliates, directors, employees and agents shall be liable to any party for any damages that might result from the use of the technology as described in this document (including without limitation direct, indirect, incidental, special, consequential and punitive damages, lost profits).

JURISDICTION AND APPLICABLE LAW

These terms shall be governed by and construed in accordance with the laws of Belgium. You irrevocably consent to the jurisdiction of the courts located in Brussels for any action arising from or related to the use of this document.

TABLE OF CONTENTS

1. SCOPE OF THE DOCUMENT 5

1.1. REFERENCES 5
1.2. CONTACTING ATOS WORLDLINE 5

2. PURPOSE OF CTAP CERTIFICATE GENERATION PROGRAM 6

3. USE OF CTAP CERTIFICATE GENERATION 7

3.1. PREREQUISITES 7
3.2. START-UP 7
3.3. DESCRIPTION 7
3.4. COMMUNICATION 8
3.5. HOW TO GENERATE A CERTIFICATE 9
3.6. ERRORS DURING EXECUTION 10
3.6.1. Validation of input data 10
3.6.2. Validation of the DEP Crypto Module 11
3.6.3. Error code from the DEP Crypto Module 11

4. ANNEX A: INSTALLATION PROCEDURE 12

5. ANNEX B: NOTATIONS 14

1. SCOPE OF THE DOCUMENT

This document describes how to generate CTAP Perso Provider and CTAP Security Scheme Provider Certificates using the *CTAP Certificate Generation* program.

The document doesn't explain the functionalities of the DEP libraries on which this program is based.

1.1. REFERENCES

This document contains references to other documents about the DEP. This paragraph gives a list of all the documents referred to.

- *DEP Host Interface Protocol*
- *DEP/Linux User Manual*
- *DEP/NMS User Manual*
- *DEP/T6 Owner's Manual*

There are no references made to the following documents, but they could be useful to understand this document.

- *DUKPT Library for DEP - Reference DFS Manual*
- *DEP Introduction to DEP*
- *DEP General Architecture*
- *DEP Glossary*

1.2. CONTACTING ATOS WORLDLINE

You can visit *Atos Worldline* on the World Wide Web to find out about new products and about various other fields of interest.
URL: www.atosworldline.com.

For the documentation visit http://www.banksys.com web page.

For support on issues related to DEP, customers, partners, resellers, and distributors can send an email to the DEP Hotline:
mailto:dephotline-atosworldline@atosorigin.com.

2. PURPOSE OF CTAP CERTIFICATE GENERATION PROGRAM

The purpose of this program is to generate CTAP Perso Provider and Security Scheme Provider certificates and put it in a specific file.

The program is intended to be used on a PC (running on Microsoft Windows 2000, Windows XP or Vista) that is connected to a DEP Platform (DEP/T6) loaded with a DEP Application Software, which can generate CTAP Certificates. It also can be added as a plug-in in DEP/NMS application.

3. USE OF CTAP CERTIFICATE GENERATION

The installation procedure is reported to the *Annex*.

3.1. PREREQUISITES

- The DEP Crypto Module must be unlocked;
- A valid DEP Application Software should be loaded on DEP Crypto Module;
- The K_DUKPT_RSA_CA key should be loaded in DEP Crypto Module;
- To use the CTAP Certificate Generation application as a DEP/NMS plug-in, the USB License Dongle must be present.

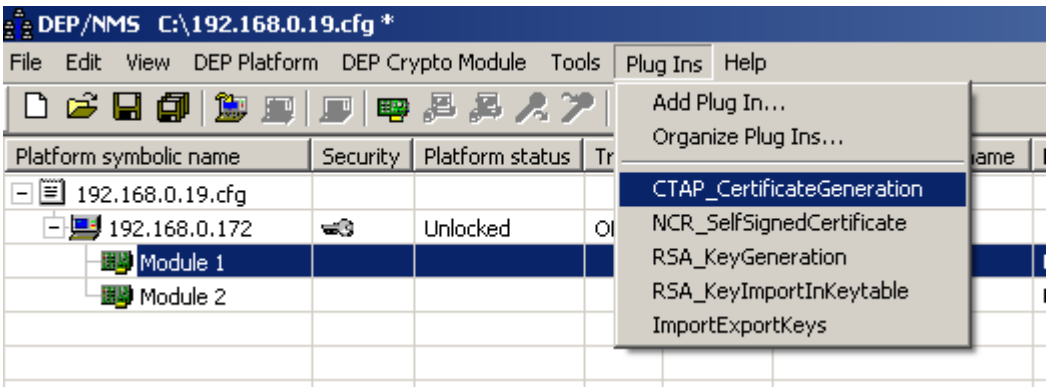
3.2. START-UP

The CTAP Certificate Generation application could be launched by executing:

C:\Program Files\Atos Worldline\DEP_NMS_PlugIns\CTAP Certificate Generation\CTAP_CertificateGeneration.exe

This is the default path. Possibly another path could be defined during the installation (paragraph 4 on page 12).

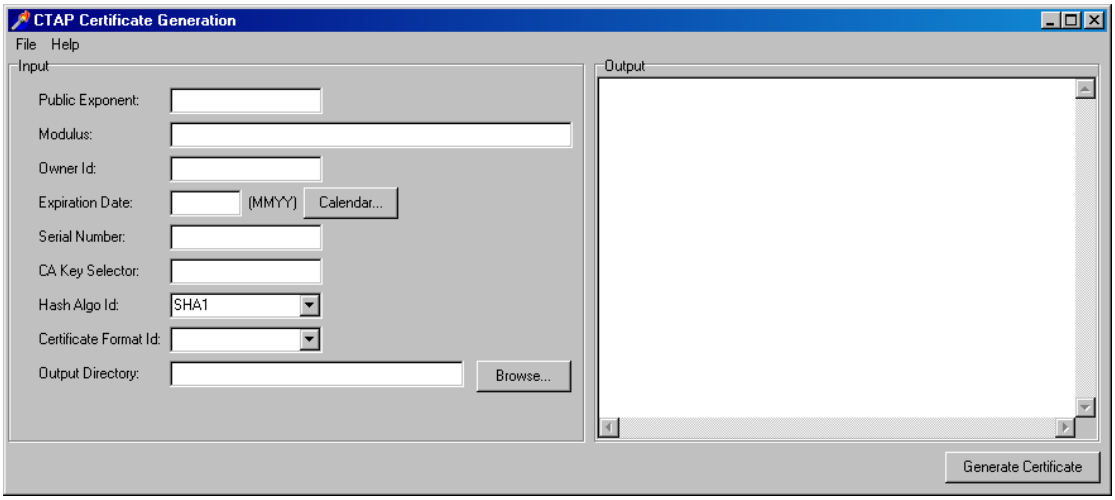
The application could also be launched directly through the DEP/NMS. Select the appropriate DEP Crypto Module and run the *CTAP_CertificateGeneration* plug-in from the **Plug Ins** menu.



Before start the application, the communication must be defined (see paragraph below).

3.3. DESCRIPTION

Once the CTAP Certificate Generation program is started, the following window is opened.

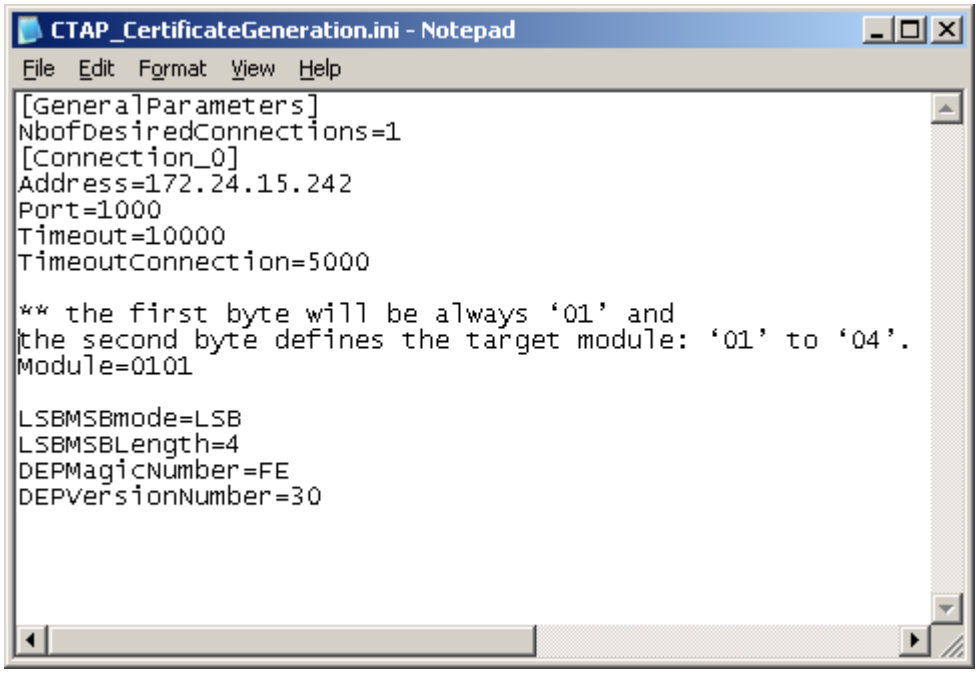


A menu at the top of the window allows to have a look at the program version (and also contact the DEP Hotline), the help files or to exit.
The Input section contains the list of parameters needed to generate a CTAP certificate (see paragraph 3.5 on page 9). The Output section (blank part) will log the operations and their results.

3.4. COMMUNICATION

If the application is launched by the *DEP/NMS*, the communication is automatically set by the *DEP/NMS* application.

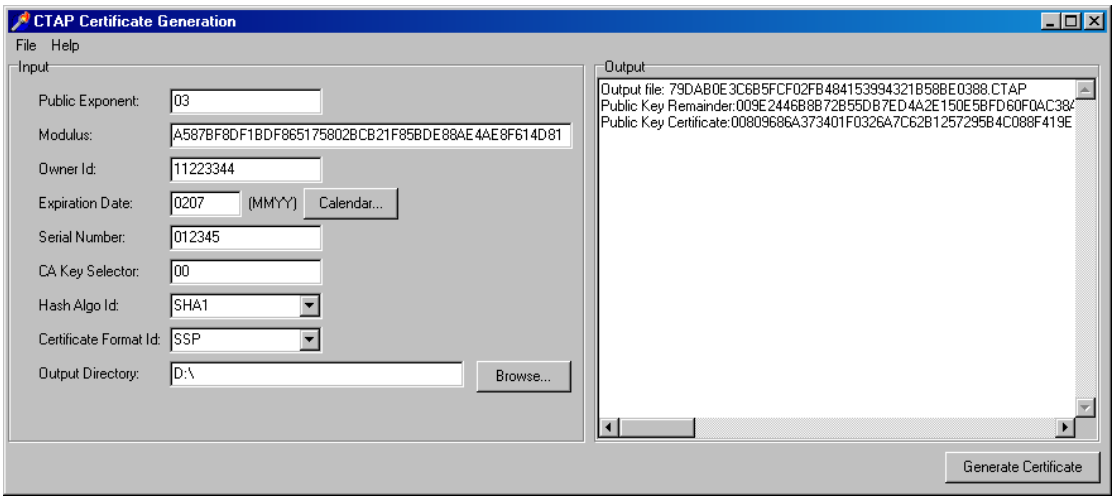
If the application is used as stand-alone application, the user should set the general parameters and the connection settings in the *CTAP_CertificateGeneration.ini* configuration file.



- *NbOfDesiredConnections* must be set to '1'.
- *Address* represents the IP address of the target platform.
- *Port* represents the TCP/IP port used for the communication with the platform.
- *TimeOut* represents the maximum waiting time in milliseconds for the response from the DEP Crypto Module.
- *TimeOutConnection* represents the maximum waiting time in milliseconds to establish the connection.
- *Module* represents the DEP Crypto Module used to generate the certificate: the first byte will be always '01' and the second byte defines the target module: '01' to '04'.
- The four last parameters are described in the *DEP Host Interface Protocol* document.

3.5. HOW TO GENERATE A CERTIFICATE

All the fields of the left panel must be filled.



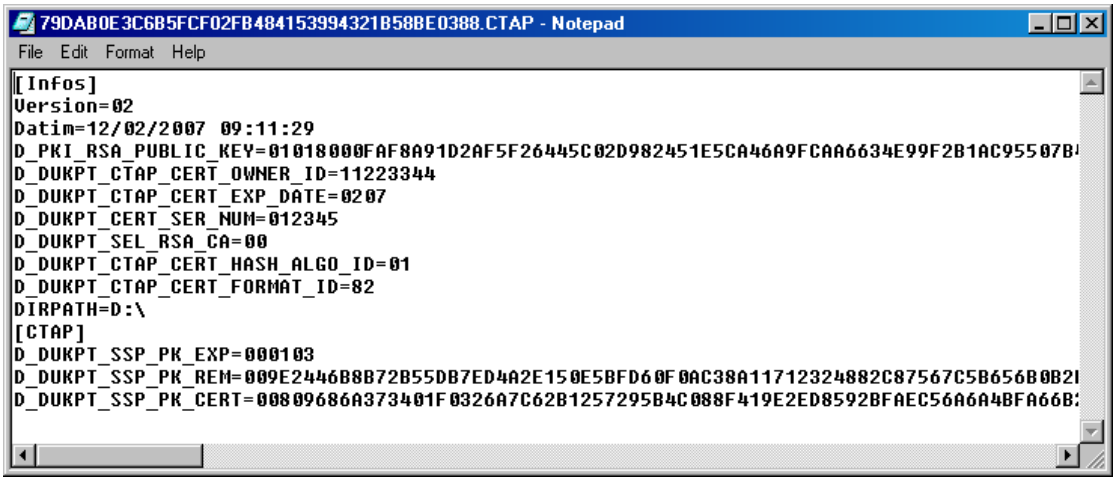
Field Name	Length	Description	Format
Public Exponent	Max 4	Public exponent for the RSA public key to be signed	b
Modulus	Max 256	Modulus for the RSA public key to be signed. (RSA 2048 bits)	b
Owner ID	4	Certificate owner ID	b
Expiration Date	2	Date after which a certificate is no longer valid. The format of the date is MMYY	n4
Serial Number	3	Certificate Serial Number	b

CA Key Selector	1	This data is used to select the right instance of the CA RSA Key in the DEP Crypto Module	b
Hash Algo ID	/	Fixed to SHA1	/
Certificate Format ID	/	Fixed to PP (Perso Provider) or SSP (Security Scheme Provider)	/
Output directory	/	Existing directory in which the certificate file will be stored.	/

When the user clicks the **Generate Certificate** button, the TCP/IP connection to the DEP Crypto Module is established and the certificate is generated.

The *Output* section shows the file name in which the certificate is stored and also the Public Key Remainder and the public key certificate.

Below is shown the structure of the CTAP certificate file.

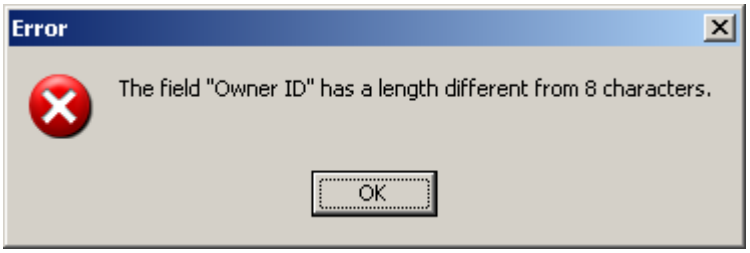


3.6. ERRORS DURING EXECUTION

3.6.1. Validation of input data

Before sending the call to the DEP Crypto Module some verifications are made and friendly messages are displayed.

For example, if the *Owner ID* field's length is different from 8 characters, the following message will be displayed.



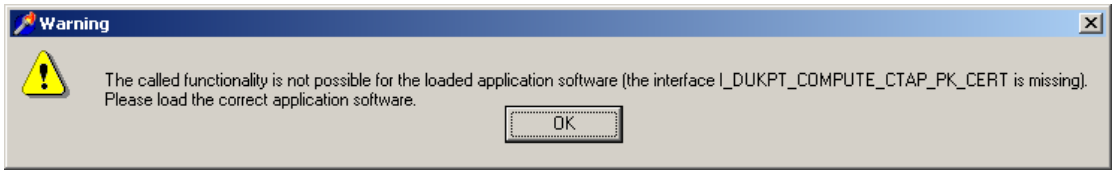
The fact that clicks on the *OK* button set the focus to the erroneous field for correction.

3.6.2. Validation of the DEP Crypto Module

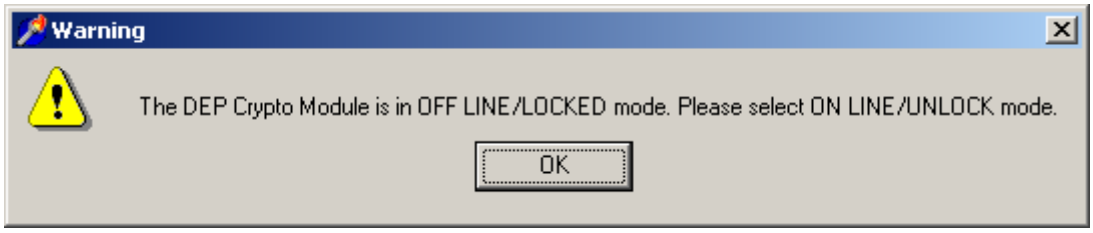
After the input validation, the application performs a DEP Crypto Module validation. The following conditions will be checked:

- If the DEP Crypto Module is on-line/unlocked;
- If the DEP Crypto Module contains a valid DEP Application Software;
- If the DEP Application Software is able to generate CTAP Certificates;
- If the CA RSA key selected by the CA Key selector present in the DEP Crypto Module.

If one of the verification failed, a warning window is displayed:


Warning
The called functionality is not possible for the loaded application software (the interface I_DUKPT_COMPUTE_CTAP_PK_CERT is missing).
Please load the correct application software.
OK

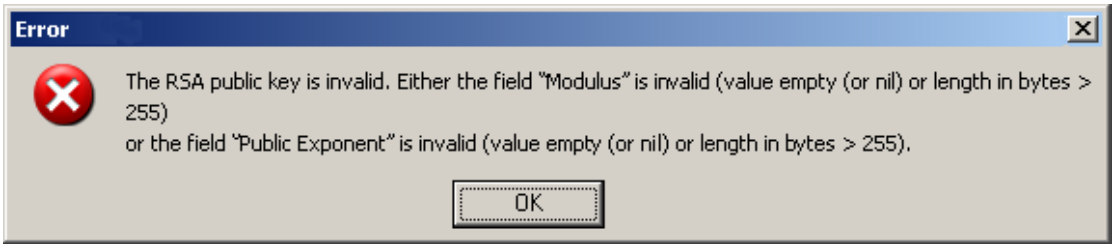
All warning windows disappear automatically when the problem is solved. For example: when the correct key is loaded or when the DEP Crypto Module is set on-line/unlocked.



3.6.3. Error code from the DEP Crypto Module

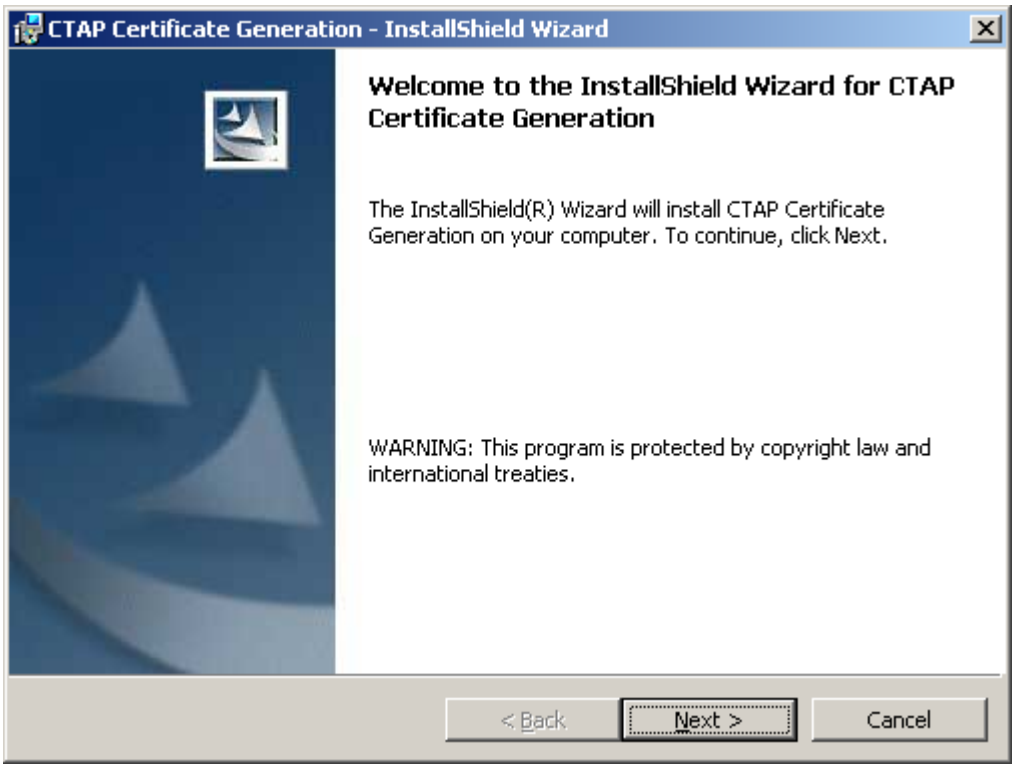
After all verifications are done successfully a call is sent to the DEP Crypto Module. If no problem occurred, the certificate will be generated; otherwise an error message will be displayed. The error refers always to the erroneous input field and gives indication for solving it.

For example:


Error
The RSA public key is invalid. Either the field "Modulus" is invalid (value empty (or nil) or length in bytes > 255)
or the field "Public Exponent" is invalid (value empty (or nil) or length in bytes > 255).
OK

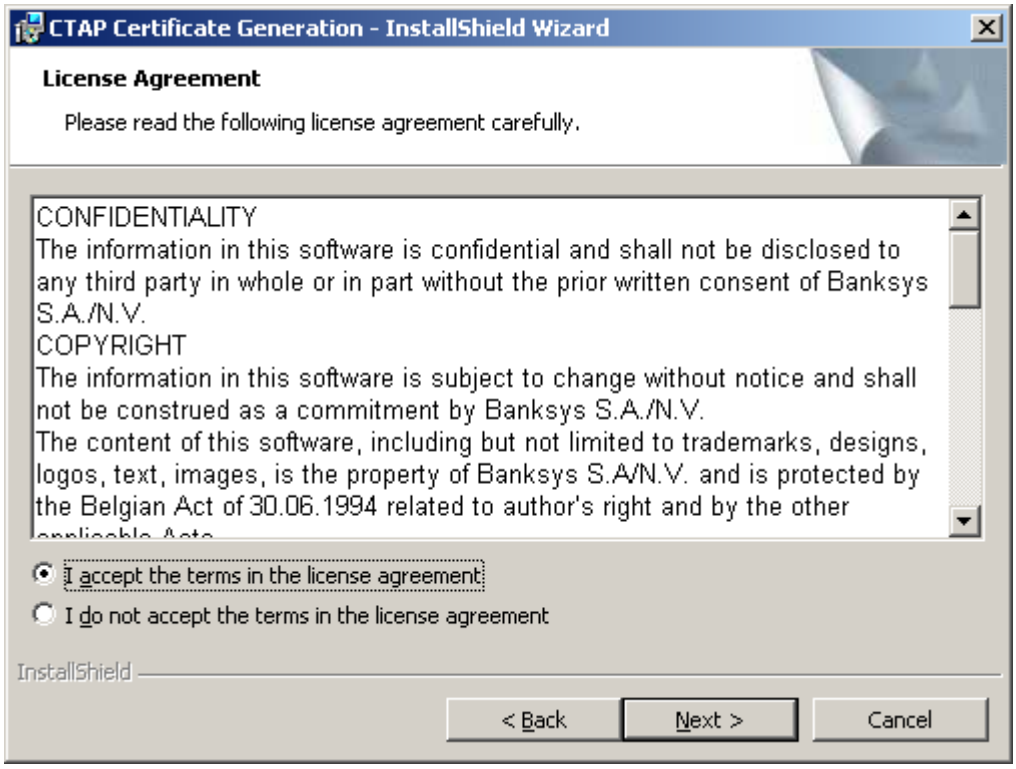
4. ANNEX A: INSTALLATION PROCEDURE

An installation procedure exists for the CTAP Certificate Generation program. It is a wizard-driven procedure that lets you to install the CTAP Certificate Generation program.
To begin the installation wizard, execute the **setup.exe**.


CTAP Certificate Generation - InstallShield Wizard
Welcome to the InstallShield Wizard for CTAP Certificate Generation
The InstallShield(R) Wizard will install CTAP Certificate Generation on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

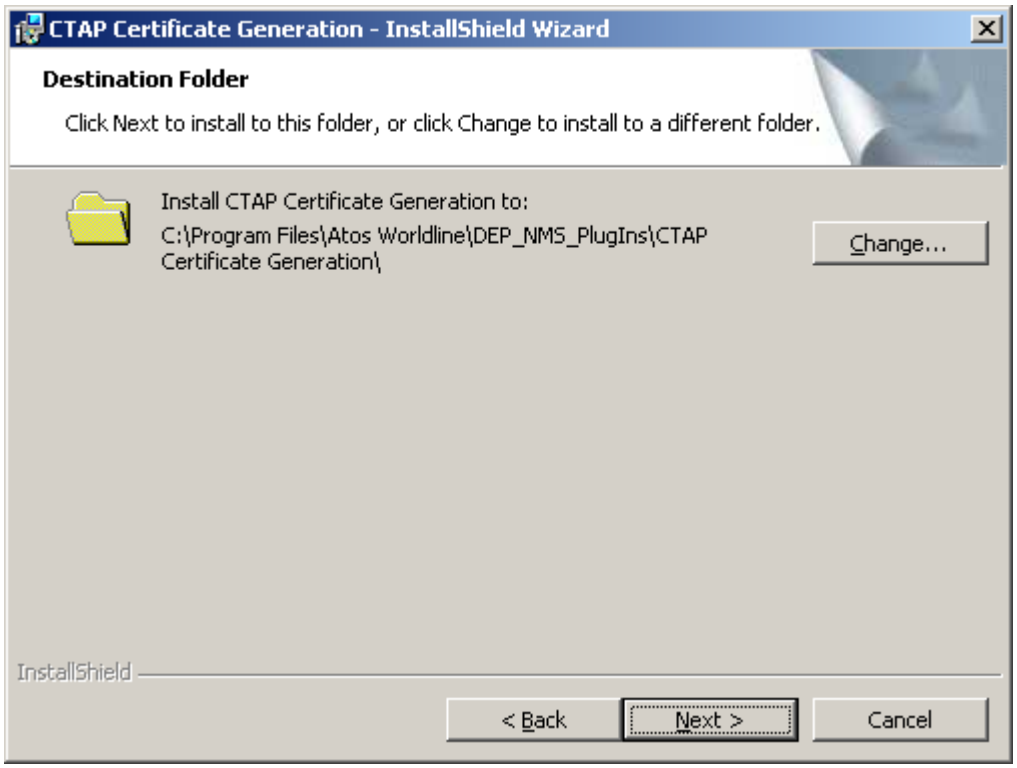
Click **Next** to continue**.**

Read and accept the License Agreement.


CTAP Certificate Generation - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
CONFIDENTIALITY
The information in this software is confidential and shall not be disclosed to any third party in whole or in part without the prior written consent of Banksys S.A./N.V.
COPYRIGHT
The information in this software is subject to change without notice and shall not be construed as a commitment by Banksys S.A./N.V.
The content of this software, including but not limited to trademarks, designs, logos, text, images, is the property of Banksys S.A/N.V. and is protected by the Belgian Act of 30.06.1994 related to author's right and by the other
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

Click the **Next** button.

The **Destination Folder** window allows defining the path where the application is installed. It is recommended to use the default path, yet you can specify a different folder by clicking **Change…** and selecting the desired folder for the installation.


CTAP Certificate Generation - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install CTAP Certificate Generation to:
C:\Program Files\Atos Worldline\DEP_NMS_PlugIns\CTAP Certificate Generation\
Change...
InstallShield
< Back
Next >
Cancel

Click **Next** to continue.
If you want to return to the previous screen, press **Back** or if you want to abort the procedure, click **Cancel.**

Once you have confirmed the installation options, the actual installation starts.

5. ANNEX B: NOTATIONS

The following abbreviations are used in this document.

b	Binary
n	Numeric